Remarks/Arguments

Reconsideration of this Application is requested.

Claims 1 and 17 have been rejected by the Examiner under 35 USC §101, because the disclosed invention is inoperative and, therefore, lacks utility. In the Examiner's opinion, Claim 1 is inoperative since no processor was claimed to run the claimed program. Claim 1 is not inoperative as the function of a processor is claimed in the following portion of claim 1.(c)(ii), which reads as follows:

> "(ii) the information storage is for posting the fee for downloading the data item from the data storage, and the buyer deposits the fund in the monetary storage prior to downloading the data item; wherein said data repository system further comprises a program capable of communicating with the data storage, the information storage and the monetary storage so as to store a fund deposited by the buyer to pay for downloading the data item into the buyer's account;"

In the Examiner's opinion, claims 1 and 17 claim functions that Applicant ascribed to digital signatures when the digital signatures are carried out by digital certificates. The definition used by the Examiner in the March 22, 2004, Final Rejection is only one of the various methods used to perform secure communications using digital signatures and certificates.

The description given by Applicant in lines 20-38 of page 6 and lines 15-20 of page 8 of Applicant's specification define the method used by Applicant to perform secure communication using digital signatures and digital certificates.

Lin s 20-28 of page 6 of Applicant's specification read as follows:

> "Preferably, the data repository system **100** is connected to a telecommunication network **120**, such as the Internet, so as to allow the users (**11-16**) to access the data repository system **100** through the telecommunication network **120**. Preferably, a Certification Authority **140** is also connected through the telecommunication network **120** so as to allow the buyer to verify the authenticity of the downloaded data items. Preferably, the Certification Authority **140** is provided by a third party who is independent of the users (**11-16**) and the data repository system **100**."

Lines 15-20 of page 8 of Applicant's specification read as follows:

> "Preferably, a digital signature of the seller is also stored in the identification code storage area **312** so that the digital signature can be provided to the buyer when the buyer downloads the data item. With the digital signature, the buyer can verify the authenticity of the downloaded data item. Similarly, a buyer may use his/her password to access the associated vault to check the balance."

Claim 1(c)(vii) and (viii) read as follows:

> "(vii) to encrypt the data item prior to downloading the data item to the buyer to prevent an unauthorized person from obtaining the downloaded data item by interception; and
>
> (viii) to provide a digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority."

Subdivision (c)(vii) of claim 1 is done so that any thing being downloaded will happen over a secure connection. Subdivision (c)(viii) of claim 1 allows an author A to place to a digital signature on this proprietary item that is being downloaded so that user U can authenticate the validity of the downloaded item. For instanc , author A posts content with a digital signature, us r U downloads author A's content from source S and validates th content using A's digital signature. In the foregoing manner, user U is sure he/she obtained author A's content and not the content prepared by a party other than author A.

The method used by Applicant as set forth in the specification to perform secure communications using digital signatures and digital certificates is also described in pages 571 and 572 of *Applied Cryptography, Second Edition* by Bruce Schneier, published by John Wiley & Sons, Inc., 1996, which reads as follows:

> "**24.6 KryptoKnight**
>
> KryptoKnight (Kryptonite - get it?) is an authentication and key distribution system designed by IBM. It is a secret-key protocol and uses either DES in CBC mode (see Section 9.3) or a modified version of MD5 (see Section 18.5). KryptoKnight supports four security services:
>
> — User authentication (called single sign-on)
> — Two-party authentication
> — Key distribution
> — Authentication of data origin and content"

Furthermore, the Examiner is not following the spirit of MPEP §2106 II when he does not reject essentially the same claim under 35 USC §101 in four prior patent office actions, i.e., April 23, 2002; August 16, 2002; January 13, 2003; and September 9,2003; and rejects this claim under 35 USC §101 in the fifth office action of March 22, 2004.

MPEP §2106 II reads as follows:

> "**II. DETERMINE WHAT APPLICANT HAS INVENTED AND IS SEEKING TO PATENT**
>
> It is essential that patent applicants obtain a prompt yet complete examination of their applications. Under the principles of compact prosecution, each claim should be reviewed for compliance with every statutory requirement for patentability n the initial review of the application, even if

> one or more claims are found to be deficient with respect to some statutory requirement. Thus, Office personnel should state all reasons and bases for rejecting claims in the first Office action. Deficiencies should be explained clearly, particularly when they serve as a basis for a rejection. Whenever practicable, Office personnel should indicate how rejections may be overcome and how problems may be resolved. A failure to follow this approach can lead to unnecessary delays in the prosecution of the application."

Claims 1, 17 and those claims dependent thereon have been rejected by the Examiner under 35 USC §112 for failing to comply with the written description requirement. The Examiner is of the opinion subdivision (c)(vii) of claim 1 to provide a digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certificate authority and subdivision (a) of claim 1, providing a digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority fails to comply with the written description requirement of 35 USC §112.

The description given by Applicant in lines 20-28 of page 6 and lines 15-20 of page 8 of Applicant's specification supply the needed written description.

The Examiner has also rejected claims 1 and 17 and those claims dependent thereon under 35 USC §112 as being indefinite for failing to particularly point out and claim the subject matter which Applicant regards as the invention. The claims refer to providing a digital signature to a buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority. The Examiner is also of the opinion that, where applicant acts as his/her own lexicographer to specifically define a term of a claim contrary t its ordinary meaning, th writt n description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the Applicant intended to so redefine that claim term.

Applicant specifically defined the terms in lines 20-28 of page 6 of Applicant's specification and lines 15-20 of page 8 of Applicant's specification.

The method used by Applicant as set forth in the specification to perform secure communications using digital signatures and digital certificates is also described in pages 571 and 572 of *Applied Cryptography, Second Edition* by Bruce Schneier, published by John Wiley & Sons, Inc., 1996.

Claims 1, 3-7, 9-17, and 19-24 have been rejected by the Examiner under 35 USC §103(a) as being unpatentable over Ginter, et al. (U.S. Patent No. 5,892,900).

Ginter discloses the following in line 66 of column 270 to line 36 of column 271.

> "A more complex form of negotiation is analogous to "haggling." In this scenario, most of the terms and conditions are fixed, but one or more terms (e.g., price or payment terms) are not. For these terms, there are options, limits and elements that may be negotiated over. A VDE electronic negotiation between two parties may be used to resolve the desired, permitted, and optional terms. The result of the electronic negotiation may be a finalized set of rules and control information that specify a completed electronic contract. A simple example is the scenario for purchasing software described above adding the ability of the purchaser to select a method of payment (VIDA, MasterCard, or American Express). A more complex example is a scenario for purchasing information in which the price paid depends on the amount of information about the user that is returned along with a usage audit trail. In this second example, the right to use the content may be associated with two control sets. One control set may describe a fixed ("higher") price for using the content. Another control set may describe a fixed ("lower") price for using the content with additional control information and field specifications requiring collection and return the user's personal information. In both of these cases,

> the optional and permitted fields and control sets in a PERC may describe the options that may be selected as part of the negotiation. To perform the negotiation, one party may propose a control set containing specific fields, control information, and limits as specified by a PERC; the other party may pick and accept from the control sets proposed, reject them, or propose alternate control sets that might e used. The negotiation process may use the permitted, required, and optional designations in the PERC to determine an acceptable range of parameters for the final rule set. Once an agreement is reached, the negotiation process may create a new PERC and/or URT that describes the result of the negotiation. The resulting PERCs and/or URTs may be "signed" (e.g., using digital signatures) by all of the negotiation processes involved in the negotiation to prevent repudiation of the agreement at a later date."

Ginter does not disclose or anticipate paragraphs (vi), (vii), and (viii) of claim 1 as amended, and those claims dependent thereon, namely, to credit the monetary sum to the seller's account, wherein the fee for downloading the data item has a range specified by the Seller and defined by a maximum amount, and a minimum amount wherein the maximum amount is the fee posted by the Seller, and a minimum amount is what the Seller is willing to collect from the buyer for downloading the data item so that the buyer is allowed to download the data item if the buyer's proposed monetary sum for downloading the data item is greater or equal to the minimum amount specified by the seller and after the buyer's proposed monetary sum is deducted from the buyer's account and credited to the seller's account; to encrypt the data item prior to downloading the data item to the buyer to prevent an unauthorized person from obtaining the downloaded data item by interception; and to provide a digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority.

Ginter also does not disclose or anticipate steps e), f), and g) of claim 17 as amended and those claims dependent thereon, namely, deducting a monetary sum from the fund and crediting the deducted sum to the seller, wherein the fee for downloading the data item in its entirety has a range specified by the Seller and defined by a maximum amount, and a minimum amount wherein the maximum amount is the fee posted by the Seller, and a minimum amount is what the Seller is willing to collect from the buyer for downloading the data item so that the buyer is allowed to download the data item if the buyer's proposed monetary sum for downloading the data item is greater or equal to the minimum amount specified by the seller; encrypting the data item prior to downloading the data item to the buyer to prevent an unauthorized person from obtaining the downloaded data item by interception; and providing a digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority.

In view of the above, claims 1, 3-7, 9-17 and 19-24 as amended are patentable. If the Examiner has any questions, would he please call the undersigned at the telephone number noted below.

Respectfully submitted,

Ronald Reichman

Ronald Reichman
Reg. No. 26,796
Attorney of Record
Telephone (203) 924-3854

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000